IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: Morris et al.

SERIAL NO.: 10/727,291 Art Unit: 2137

FILED: 12.03.2003 EXAMINER:Williams, Jeffrey

FOR: METHOD AND SYSTEM FOR INCREASING DATA ACCESS IN A SECURE SOCKET LAYER NETWORK ENVIRONMENT

APPEAL BRIEF 37 CFR 41.37

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST (37 CFR 41.37(c)(1)(i))

The real party in interest is Stampede Technologies, Inc.

Stampede Technologies, Inc. is a leader in software development in the area of accelerating data over various networks. Numerous independent articles recognize Stampede Technologies, Inc. as a leader in the field of enhancing communication over networks, such as the Internet, see for example,http://www.businesswire.com/portal/site/home/permalink/?ndmViewId=news_view&newsId=20100628005866&newsLang=en, http://www.newcom-intl.com/index.php/news/67-newcom-international-selects-stampede-technologies-new-fx-series-for-satellite-wan-optimization-.html.

II. RELATED APPEALS AND INTERFERENCES (37 CFR 41.37(c)(1)(ii))

On information and belief, there are no related appeals or interferences to the above-identified application.

III. STATUS OF CLAIMS (37 CFR 41.37(c)(1)(iii))

Claims 1, 2, 9, 11, 12, 19, 24, 25 and 26 stand rejected.

Claims 1, 2, 9, 11, 12, 19, 24, 25 and 26 are appealed.

IV. STATUS OF AMENDMENTS (37 CFR 41.37(c)(1)(iv))

The Amendment of April 16, 2010 after final has not been entered or fully considered, but was within the advisory period and is believed in condition to be entered in view of the record.

V. SUMMARY OF CLAIMED SUBJECT MATTER (37 CFR 41.37(c)(1)(v))

The invention is summarized by referring to the specific parts of the specification and drawings.

Independent Claim 1.

A system (FIG. 2A, page 6 lines 1-22, page 7, lines 1-22 and page 8, line 1) for increasing data access in a secure socket layer network environment includes a web server computer (102) having SSL protocol server software operably associated therewith for enabling a first SSL connection, wherein SSL protocol server software includes a CA certificate and private key (page 6 lines 3-7), SSL acceleration server software operably associated with the web server computer which includes a pseudo CA certificate and access to the private key and a public key (page 6 lines 14-18). A client computer 104 (FIG. 2A,) is communicatively linked to the web server computer (102) having web browser software having SSL protocol client software operably disposed thereon for enabling the first SSL connection between the client computer and the web server (page 6 lines 8-11), wherein the first SSL connection is established between the web browser software and SSL acceleration client software operably disposed thereon the client computer, and wherein the SL connection (page 6 lines 19-22, page 7, lines 1-22 and page 8, line 1).

Dependent claim 2.

The SSL acceleration client software is further equipped for monitoring when the web browser requests the first SSL connection with the web server computer and intercepting the SSL request from the web browser, and diverting communication through the second SSL connection (FIG. 2A and 2B, page 6 lines 11-21).

Dependent claim 9.

Also provided is compression software (page 7, lines 17 and 18) for transmitting data secure communications between the client computer and the web server computer over the second SSL connection.

Independent claim 11.

A method for increasing data access in a secure socket layer network environment (FIG. 2A, FIG. 2B) includes the steps of employing a web server computer (102) having SSL protocol server software operably associated therewith for enabling a first SSL connection (page 6 lines 3-7), wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with the web server computer which includes a pseudo CA certificate and access to the private key and a public key (page 6 lines 14-18); and

employing a client computer (104) communicatively linked to the web server computer (102) having web browser software having SSL protocol client

software operably disposed thereon for enabling the first SSL connection between the client (104) and the web server (102), wherein the first SSL connection is established between the web browser software and SSL acceleration client software operably disposed thereon residing with the client computer, wherein the SSL acceleration client software communicates with the SSL acceleration server software to receive a copy of the pseudo CA certificate and the public key and present the pseudo CA certificate to the web browser software through SSL acceleration server software for validation thereof for enabling a second SSL connection with the first SSL connection between the client computer and the web server computer, wherein the second SSL connection is established between the SSL acceleration client software and the SSL acceleration server software in a manner wherein the private key is never transmitted to the SSL acceleration client software on the client computer and which permits optimization techniques to be applied on data transmitted through the second SSL connection (page 6 lines 19-22, page 7, lines 1-22 and page 8, line 1, FIG. 2A and 2B).

Dependent claim 12.

The SSL acceleration monitors when the web browser requests the first SSL connection with the web server computer and intercepts the SSL request from the web browser, and diverts communication through the second SSL connection. (FIG. 2A and 2B, page 6 lines 11-21)

Dependent claim 19.

The method includes employing compression software (page 7, lines 17 and 18) for transmitting data secure communications between the client computer and the web server computer over the second SSL connection.

Independent claim 24.

A system for increasing data access in a secure socket layer network environment, which includes:

a web server computer (102) having SSL protocol server software operably associated therewith for enabling a first SSL connection (FIG. 2A, FIG. 2B) (page 6 lines 3-7) wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with the web server computer which includes a pseudo CA certificate and access to the private key and a public key (page 6 lines 14-18) and

a second computer (104) communicatively linked to the web server computer (102) operably associated with web browser software having SSL protocol client software operably disposed thereon for enabling the first SSL connection between a client computer (104) and the web server (102), wherein the first SSL connection is established between the web browser software and SSL acceleration client software operably disposed thereon the second computer (104), wherein the SSL acceleration client software communicates with the SSL acceleration server software to receive a copy of the pseudo CA certificate and the public key and present the pseudo CA certificate to the web browser software

for validation thereof for enabling a second SSL connection with the first SSL connection between the client computer and the web server computer, wherein the second SSL connection is established between the SSL acceleration client software and the SSL acceleration server software in a manner wherein the private key is never transmitted to the SSL acceleration client software and which permits optimization techniques to be applied on data transmitted through the second SSL connection (page 6 lines 19-22, page 7, lines 1-22 and page 8, line 1, FIG. 2A and 2B).

Dependent claim 25.

The SSL acceleration client software is further equipped for monitoring when the web browser requests the first SSL connection with the web server computer and intercepting the SSL request from the web browser, and diverting communication through the second SSL connection. (FIG. 2A and 2B, page 6 lines 11-21)

Dependent claim 26.

The system includes compression software (page 7, lines 17 and 18) for transmitting data secure communications between the client computer and the web server computer over the second SSL connection.

VI. GROUND OF REJECTIONS TO BE REVIEWED ON APPEAL (37 CFR 41.37(c)(1)(vi))

Whether the specification and claims 1, 2, 9, 11, 12, 19, 24, 25 and 26 fail to comply with the written description requirement under 35 U.S.C. § 112, first paragraph.

Whether claims 1, 2, 9, 11, 12, 19, 24, 25 and 26 are unpatentable under 35 U.S.C. §103(a) as obvious over United States Patent No 6643701 to Aziz et al. in view of United States Publication 2003/0046532 to Gast and/or in view of Freed et al. United States Publication 2003/0014628.

VII ARGUMENT (37 CFR 41.37(c)(1)(vii))

An issue before the Board is whether the specification and claims 1, 2, 9, 11, 12, 19, 24-26 fail to comply with the written description requirement under 35 U.S.C. § 112, first paragraph, as concluding with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

The Examiner's Rejections under 35 U.S.C §112

In response to final Office Action dated 11/10/2009, applicant amended the claims which the Examiner indicated triggered a rejection under 35 U.S.C. § 112 second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Specifically, the examiner stated:

Claims 1, 2, 9, 11, 12, 19, 24-26 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 1, 11, and 24, the examiner notes that the amended recitations of "operably residing therewith" and "operably residing with" lack antecedent basis within the applicant's disclosure. The examiner respectfully reminds the applicant that claims must conform to the invention as set forth in the remainder of the specification and the terms and phrases used in the claims must find clear support or antecedent basis in the description so that the meaning of the terms in the claims may be ascertainable by reference to the description (see 37 CFR § 1.75). In the instant case, the examiner points out that the recitations in question render the claims ambiguous and the applicant's specification fails to

provide clear direction as to their interpretation.

For example, the examiner points out that it is unclear whether the applicant's use of "operably residing" with/therewith is an attempt to reference a physical location of software or a reference to the software's state of cooperation or dwelling in league with the computer. The examiner further points out that applicant's remarks fail to address these amended recitations. The examiner notes that the applicant's original disclosure states that each of the various software modules or components (e.g. SSLAC, SSLAS) may be physically located or off-loaded onto one or more intermediary devices within the system (i.e. the SSLAC and SSLAS are located on an intermediary computer with the system - Specification, pg. 8). Thus, the examiner notes that the recitation "operably residing" with/therewith would appear to properly be interpreted as reference to the software components' or modules' state of cooperation with the rest of the system components as opposed to a reference of a particular physical location of the components.

Regarding claims 1 and 11, the examiner notes that the recitation "the SSL acceleration client software on said client computer" (claim 1, line 19; claim 11, line 19, 20) lacks antecedent basis within the claim terminology. For the purpose of examination, the examiner presumes the applicant to recite "the SSL acceleration client software operably residing with said client computer".

All depending claims are rejected by virtue of dependency.

Applicants filed an after final amendment on March 4, 2010, which amended the claims to state “disposed thereon” as opposed to “residing therewith” and this language is clearly in the specification, page 5, lines 10 and11 and in the drawings see FIG. 2A, for example. In an advisory action in response to the after final amendment the Examiner maintained that the change would require further searching and consideration. The change deals with the web browser software having SSL protocol client software operably disposed on the client computer and the change was made to be consistent with the language in the specification per the examiner’s prior comments to use such language in lieu of the “residing therewith” language. The examiner’s position is that the change

and arguments would not result allowance of the case as examiner stated "Applicants' arguments have been found unpersuasive."

As such, Applicants would find themselves back before the Board to address the substantive § 103 issues. Applicants submit that the proposed amendment is well founded and that the change is one of semantics in relation to raising an issue which would require a new search and further consideration and would not require the examiner to do so. The amendment is submitted to be proper and is believed to overcome the prior 112 rejection and reversal of the rejection is requested.

Rejections under 35 U.S.C § 103

An issue before the Board is whether claims 1, 2,11, 12, 24 and 25 are unpatentable under 35 U.S.C. §103(a) as obvious over United States Patent No 6643701 to Aziz et al. in view of United States Publication 2003/0046532 to Gast.

Another issue before the Board is whether claims 9, 19 and 26 are unpatentable under 35 U.S.C. §103(a) as obvious over United States Patent No 6643701 to Aziz et al. in view of United States Publication 2003/0046532 to Gast and/or in view of Freed et al. United States Publication 2003/0014628.

The Nonobviousness Requirement under 35 U.S.C. §103 states a patent may not be obtained though the invention is not identically disclosed or described as set forth title 35 USC § 102, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a

whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The Supreme Court recently addressed the issue of obviousness in KSR International Co. v. Teleflex Inc., 127 S. Ct. 1727 (2007). The Court stated that the Graham v. John Deere Co. of Kansas City, 383 U.S. 1 (1966), factors still control an obviousness inquiry. Those factors are: 1) "the scope and content of the prior art"; 2) the "differences between the prior art and the claims"; 3) "the level of ordinary skill in the pertinent art"; and 4) objective evidence of nonobviousness. KSR, 127 S. Ct. at 1734 (quoting Graham, 383 U.S. at 17-18). Moreover, the Court indicated that there is "no necessary inconsistency between the idea underlying the TSM test and the Graham analysis." Id. As long as the test is not applied as a "rigid and mandatory" formula, that test can provide "helpful insight" to an obviousness inquiry. KSR, 127 S. Ct. at 1731; Takeda Chemical Industries, Ltd. v. Alphapharm Pty., Ltd., No. 06-1329 (Fed. Cir. June 28, 2007). It is also stated that "where an application claims a structure already known in the prior art that is altered by the mere substitution of one element for another known in the field, the combination must do more than yield a predictable result". KSR, at 1739. In other words, if a person of ordinary skill can implement a predictable variation of known components, § 103 likely bars its patentability. KSR was concerned with substitution of a known component having a known function and substituting it into another invention for performing the same

function, i.e., a predictable result.

Prior Art at time of the Invention

The cited art references in this case are United States Patent No. 6643701 to Aziz et al. in view of United States Publication 2003/0046532 to Gast and in view of Freed et al. United States Publication 2003/0014628. No other reference is cited in combination therewith to render obvious the claims.

Prior to the claimed invention, the prior art provided for establishing a single SSL connection between a same client and server pair through which an established communication transmitted data over such connection using an established certificate. Each prior art paradigm fails to show multiple SSL connections established between the same client and server wherein a given certificate and a copy of the certificate are employed in a manner as claimed in the instant invention.

Aziz only discloses making a single connection between each client and a relay and a relay and a server. Aziz states that the connection can be a cleartext HTTP connection (non-secure).

Gast is directed to a system and method for accelerating cryptographically secured transactions. Gast is concerned with offloading encryption processing to central encryption servers equipped with hardware built to accelerate encryption speed and reduce encryption latency. Gast is concerned with offloading encryption processing to central encryption servers equipped with hardware built to accelerate encryption speed and reduce latency [see paragraph 0015 of Gast].

Gast simply moves the task of processing the security mechanism, i.e., establishing a SSL session to a central control point [0022]. The point stressed in Gast is to offload the establishment of SSL connections by the server, not to establish additional SSL connections between the same client and server pairing. In contrast, the instant invention provides a CA certificate and a pseudo CA certificate to establish concurrent SSL connections whereby data can pass in a compressed form, for example, in the second established connection.

Freed et al. discloses a secure sockets layer architecture which employs an intermediate device between the client computer and the server computer which intercepts SSL/TCP data and then performs one or more transactions to aid in acceleration. Freed et al. only acts as an intermediary intercepting all communication over the existing SSL connection and passes the data accordingly, paragraph [0039]. Paragraphs [0052] - [0053] and the claims in Freed et al. further illustrate Freed et al. are only concerned with providing a classic SSL connection between the client and server through an intermediary device.

Differences between the Claimed Invention and Art

Neither Aziz, Gast or Freed et al. alone or together disclose, suggest or teach the invention nor do any provide a teaching, suggestion or motivation to perform the method of instant claimed invention. It is only the Examiner's opinion as to what the cited references teach, suggest or disclose and this has been

refuted by Applicants specifically pointing out the scope of the art, differences between the references and the instant invention and the level of skill in the art at that time.

Aside Aziz, Gast or Freed et al. which Applicants assert do not teach, disclose or suggest the invention, no other evidence has been put forth which teaches, suggests or discloses the invention. Applicants provided adequate evidence to rebut the examiner's contention via arguments of record.

In addressing the first factor cited above, it is respectfully submitted that the cited art, namely, Aziz, Gast or Freed et al., do not render obvious the instant invention, to produce the claimed present invention. A person of ordinary skill in the field for making a system or method of using a system for increasing data access in a secure socket layer network environment as with the instant invention at the time of the invention would not have reasonably looked at Aziz, Gast nor Freed et al. and been able to derive the claimed invention. Combining Aziz, Gast or Freed et al. teachings at best provide for a system for offloading encryption latency issues using single SSL connections between a server, relay and client computer. As can be seen from their combined specification and claims, this does no more than teach of single conventional SSL connection techniques between the same client and server pairing using a single given certificate.

The Examiner failed to correctly appreciate and consider all of the limitations in the claimed invention as seen in the attached claims hereto as

properly interpreted in light of the applicants' specification. Rather, the Examiner has composed an incomplete set of pieces of art in an effort to assemble a system to render an obviousness rejection. However, no cutting and pasting of such pieces can in any way do so.

Aziz only discloses making a single connection between each client and a relay and a relay and a server. Aziz states that the connection can be a cleartext HTTP connection. This, however, can be a problem and create a security issue because Basic credentials are Base64-encoded. If Basic credentials are sent over an HTTP connection, they may be read as clear text and decoded. This destroys the whole notion of the SSL paradigm.

Gast chooses to offload the cryptographic process to central cryptographic hardware component employing an intermediary device to deal with the issue as opposed to creating an additional potential encryption latency issue between a server and client.

In Freed et al. there is no direct link between the client computer and the server computer. As seen in paragraphs [0007-0010] of Freed et al., there is merely a conventional SSL handshake which is employed and all secure data is sent through the one secure tunnel which is created. Freed et al. are concerned with offloading the server the task of encryption/decryption task by employing a tertiary or intermediary device to interact with the client and the server. The tertiary computer employs conventional handshake technology.

In the instant invention, the SSL acceleration client software communicates

with the SSL acceleration server software to receive a copy of the pseudo CA certificate and the public key and present the pseudo CA certificate to the web browser software through SSL acceleration server software for validation thereof (thus putting communications in the clear) for enabling a second SSL connection with the first SSL connection between the client computer and the web server computer, wherein the second SSL connection is established between the SSL acceleration client software and the SSL acceleration server software in a manner wherein the private key is never transmitted to the SSL acceleration client software on the client computer and which permits optimization techniques to be applied on data transmitted through the second SSL connection. The SSL connection is terminated (completed) at the client computer by the SSL acceleration client software (SSLAC) using the credentials of the content server's certificate for the purpose of putting the SSL transactions in the clear so that advanced data compression and elimination of application level handshakes can be performed over a second SSL communication link (or tunnel) between the SSLAC and the SSL acceleration server software (SSLAS).

Here, the applicant points out quite clearly that the art cited is deficient in lacking the claimed structure or a known function or predictable result. There are indeed claimed differences between the prior art and the claims. At the time of the invention, the level of skill in the art has not been shown to have developed as to the art of SSL acceleration client software (SSLAC) on a client computer which communicates with the SSL acceleration server software (SSLAS) to

receive a copy of a pseudo CA certificate and the public key and present the pseudo CA certificate to the web browser software for validation thereof for enabling a second SSL connection with the first SSL connection between the client computer and the web server computer, wherein the second SSL connection is established between the SSL acceleration client software and the SSL acceleration server software in a manner wherein the private key is never transmitted to the SSL acceleration client software on the client computer and which permits optimization techniques to be applied on data transmitted through the second SSL connection. By so doing, the SSL connection is terminated (i.e., connected) at the client computer by the SSL acceleration client software (SSLAC) using the credentials of the content server's certificate for the purpose of putting the SSL transactions in the clear so that advanced data compression and elimination of application level handshakes can be performed over a second SSL communication link (or tunnel) between the SSLAC and the SSL acceleration server software (SSLAS). No like structure is found in the cited art.

The only evidence of record which has been offered at this time tilts toward patentability. The Court held in Graham v. John Deere Co., 383 U.S. 1 (1966):

> While the ultimate question of patent validity is one of law, ... the § 103 condition, which is but one of three conditions, each of which must be satisfied, lends itself to several basic factual inquiries. Under § 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or nonobviousness of the subject matter is determined. Such secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the

origin of the subject matter sought to be patented. As indicia of obviousness or nonobviousness, these inquiries may have relevancy.

This is not to say, however, that there will not be difficulties in applying the nonobviousness test. What is obvious is not a question upon which there is likely to be uniformity of thought in every given factual context. 383 U.S. at 17-18 (citations omitted).

The Court also instructed that the standard set forth in Graham would go beyond an inquiry of purely technical issues:

These legal inferences or subtests do focus attention on economic and motivational rather than technical issues and are, therefore, more susceptible of judicial treatment than are the highly technical facts often present in patent litigation.... Such inquiries may lend a helping hand to the judiciary which, as Mr. Justice Frankfurter observed, is most ill-fitted to discharge the technological duties cast upon it by patent legislation. …They may also serve to "guard against slipping into use of hindsight," … and to resist the temptation to read into the prior art the teachings of the invention in issue. 383 U.S. at 35-36 (citations omitted).

Stated Grounds of Rejection by Examiner under 35 U.S.C § 103 and Response

In the Final Office Action dated 3-4-2010, the Examiner stated:

> Regarding claim 24, the examiner notes that Aziz discloses a system, comprising a client, server, and intermediary devices for establishing first (fig. 4:410) and second (fig. 4:460) SSL connections between a client and a server. The system comprises software components of SSL protocol server software" (Aziz, 6:21-24) and SSL protocol client software" (Aziz, 6:18-21) . However, Aziz does not appear to discuss the notion of SSL acceleration. Therefore, Aziz does not appear to disclose the recited software components of SSL acceleration server software and SSL acceleration client software.
>
> Gast discloses the advantage of employing software components for SSL acceleration upon an intermediary device within a system for enabling SSL connections between a client and server. It would have been obvious to one of ordinary skill in the art to recognize the benefits of acceleration as disclosed by Gast within the system of Aziz. This would have been obvious because one of ordinary skill in the art would have been motivated by the advantages of speed and efficiency" The combination of Aziz and Gast

enable [the claimed invention].

Applicants respectfully traverse. The object of both Aziz and Gast inventions is to provide a system wherein acceleration is an encryption offload service. That is, there is a front- end server which introduces an efficiency by performing encryption in hardware and offloading the content server.

This has absolutely nothing to do with the efficiency taught by the instant invention, in which the SSL connection is terminated (completed) at the client computer by the SSL acceleration client software (SSLAC) using the credentials of the content server's certificate for the purpose of putting the SSL transactions in the clear so that advanced data compression and elimination of application level handshakes can be performed over a second SSL communication link (or tunnel) between the SSLAC and the SSL acceleration server software (SSLAS). In the instant invention, the SSL acceleration client software communicates with the SSL acceleration server software to receive a copy of the pseudo CA certificate and the public key and present the pseudo CA certificate to the web browser software through SSL acceleration server software for validation thereof (thus putting communications in the clear) for enabling a second SSL connection with the first SSL connection between the client computer and the web server computer, wherein the second SSL connection is established between the SSL acceleration client software and the SSL acceleration server software in a manner wherein the private key is never transmitted to the SSL acceleration

client software on the client computer and which permits optimization techniques to be applied on data transmitted through the second SSL connection.

In the Aziz/Gast cases, the acceleration is merely taught to be an encryption offload service. In the instant invention the actual data communications between the client and the data center is optimized. This is a fundamental difference which is not taught by either Aziz or Gast.

To Claim 1, the Examiner asserts Aziz discloses first and second SSL connections between a client and server and a web server computer having SSL protocol server software as claimed and a client computer having web browser software having SSL protocol software as claimed, but does not include SSL acceleration software and cites Gast in this regard. It is asserted that it would have been obvious to one skilled in the art to recognize the benefits of acceleration of Gast within the system of Aziz.

The examiner goes on to state:

The combination of Aziz and Gast enable a web server having SSL protocol server software operably associated therewith for enabling a first SSL connection, wherein SSL protocol server software includes a CA certificate and private key (fig 3:340, 4:470; 6:21-25; 5:6-13) , SSL acceleration software operably associated with said web server computer (Gast, fig 2:214; par. 34; Aziz, fig. 4:440; 5:6-13) which includes a pseudo CA certificate and access to said private key and a public key. Herein, the combination enables an intermediary comprising server acceleration software with access to the server's private key, certificate and a public key for the purpose of functional acceleration within SSL.

and a second computer communicatively linked to said web server computer (Aziz, fig. 4:420) operably associated with web browser software having SSL protocol client software operably residing (Aziz, 6:18-21 herein Aziz discloses a client comprising software for enabling an SSL connection) therewith for enabling said first SSL connection between a client computer and said web

server computer, wherein said first SSL connection is established between said web browser software and SSL acceleration client software operably residing with said client computer (Aziz, fig 4:420) wherein said SSL acceleration software communicates with said SSL acceleration server software to receive a copy of said pseudo CA certificate and said public key and present said pseudo CA certificate to said web browser software for validation thereof (Aziz, 5:6-13, 41-65) for enabling a second connection (Aziz, fig. 4:460) with said first SSL connection (Aziz, fig. 4:410) between said client computer and said web server computer, wherein said second SSL connection is established between SSL acceleration client software and said SSL acceleration server software in a manner wherein said private key is never transmitted to the SSL acceleration client software on said client computer (Aziz, 5:4-7 - herein, Aziz discloses that the server shares its private key with the "SSL acceleration server software" (e.g. relay) but not the "SSL acceleration client software" (E.g. proxy), and which permits optimization techniques to be applied on data transmitted through said SSL connection (Gast, fig 2:202, 214, 206, 212).

Again, the Gast figure cited teaches a cryptographic acceleration method. Aziz is teaching the same. Neither is teaching what is taught by the instant invention, in which the SSL connection is terminated at the client computer by the SSLAC using the credentials of the content server's certificate for the purpose of putting the SSL transactions in the clear so that advanced data compression and elimination of application level handshakes can be performed over a second SSL tunnel between the SSLAC and the SSLAS. This is simply not taught at all by either Gast or Aziz.

The Examiner states:

Regarding claim 25, the combination enables: wherein said SSL acceleration client software is further equipped for monitoring when said web browser requests said first SSL connection with said web server computer and intercepting said SSL request from said web browser, and diverting communication through said second SSL connection (Aziz, 5:49-56; 8:66-9:13).

Aziz 5:49-56; 8:66-9:13 does not teach putting the traffic between the client computer and the proxy in the clear. It does teach putting the traffic between the relay and the web server in the clear, which is the point of the cryptographic offload.

In contrast, the applicant's instant invention does put the SSL traffic in the clear for the purposes of injecting advanced data compression and elimination of application level handshakes can be performed over a second SSL tunnel between the SLAC and the SLAS. This is not taught, suggested or disclosed by the art in any way.

The examiner states:

“Regarding claims 9, 19 and 26, the combination recites software for transforming SSL data transmissions, but does not appear to explicitly recite compression.”

Applicants’ response to this: Of course it doesn't recite compression because the purpose of the cited art is to inject an encryption offload service in order to reduce the load on the web content server, whereas the purpose of the instant invention, which unlike the inventions cited, puts the SSL traffic in the clear for the purposes of injecting advanced data compression and elimination of application level handshakes which can be performed over a second SSL tunnel between the SLAC and the SLAS. Nowhere in the cited invention is that sort of "transformation" taught.

The examiner states:

“Freed, however teaches that SSL data transmissions are transformed by compression (Freed, par 10,52).”

Here, the examiner is latching on to Freed's writings that a "compression method" is one of the negotiated aspects when setting up an SSL connection. The applicant is aware that a compression method is part of the SSL negotiations. However, one skilled in the art would realize that there is much more to advanced data communications optimization than negotiating a compression method. Since a compression method has always been a basic part of SSL handshaking negotiations, the instant invention would be completely unnecessary if this compression method provided all the benefits of the instant invention.

The reality is that there is a need for more sophisticated compression than that which is inherent in SSL and in fact the built-in compression methods which can be negotiated in an SSL handshake are rarely used. The instant invention provides more sophisticated compression method which include not only reduction of data transfer but also elimination of application level hand-shakes. The fact that Freed cites a well-known facet of SSL communications is irrelevant since SSL is a fundamental part of the operating environment of the instant invention. Freed (like Aziz and Gast) does not teach putting the SSL traffic in the clear for the purposes of injecting advanced data compression and elimination of application level handshakes which can be performed over a second SSL connection between the SLAC and the SLAS.

Notably, there is no teaching wherein the second SSL connection is established between the SSL acceleration client software and the SSL acceleration server software in a manner wherein the private key is never transmitted to the SSL acceleration client software and which permits optimization techniques to be applied on data transmitted through the second SSL connection.

The examiner states:

> It would have been obvious to one of ordinary skill in the art to employ compression within the SSL data transmission of the combination of Aziz and Gast. This would have been obvious because one of ordinary skill in the art would have been motivated by the teachings of the prior art regarding the nature of SSL transmissions.

This might be if the cited inventions can simply negotiate the data compression features of SSL, which simply compresses the payload as part of the encryption process. However, advanced data compression techniques require putting the data in the clear at the client. Unlike the prior art which completely lacks such teaching, the instant invention provides advanced data compression techniques which include functions like cache differencing and elimination of application level handshakes. None of the art cited teach putting the SSL traffic in the clear to enable performing such compressed data transmission by means of providing the claimed instant invention.

The examiner argues that it is applicants' position that the prior art only suggests forming multiple SSL connections wherein the CA certificate including

all components access to the private key and a public key exist in each instance of forming such connections which however in so doing would violate the SSL paradigm in the case of performing data optimization operations between a server and client. In contrast, the instant invention does not transmit the private key to preserve the SSL paradigm and yet enables optimization techniques to be performed through the second SSL connection between client and server.

As to the Examiner's remarks, the above statement by the examiner is not an accurate assessment of what was argued in the Applicant and Examiner's prior interview which took place in December 2009. At the interview it was stated that the private key is never transmitted from the SSLAS to the SSLAC. The teachings of the instant invention make it abundantly clear the private key is made accessible to the SSLAS, otherwise the instant invention would be implausible.

The examiner states:

The examiner respectfully notes that the applicant's new and amended claims appear to recite a system comprising a client, server, and one or more intermediary devices for enabling the recited "first SSL connection" and "second SSL connection" The applicant asserts that "the instant invention does not transmit the private key", however the examiner respectfully points disagrees. It is noted that the instant invention does in fact transmit or share the private key of the server with the intermediary SSLAS. Thus, the applicant's invention does not appear to distinguish over the prior art's disclosure of sharing the private key with the SSLAS (i.e "relay) (Aziz, 5-17).

To this, Applicants responds as follows. The teachings of the instant invention make it very clear that the private key is shared between the SSLAS

and the content server. However what distinguishes the instant invention between the prior art cited and all other known prior art, is that the instant invention is able to terminate (complete) the SSL connection at the client using the credentials of the web server but without transferring the private key over to the client. This key distinguishing function is implemented without violating the SSL paradigm because all of the underlying communications which make this feat possible are done through the second SSL connection , i.e., the second SSL connection has been further characterized to be formed in a manner wherein the private key is never transmitted to the SSL acceleration client software on the client computer. This is not taught anywhere but in the instant invention.

The references were discussed as lacking the now claimed structure. Namely, there is no disclosure, suggestion or teaching in the art, alone or in combination, of the system or method now recited.

The claimed invention is not shown, taught or suggested in the prior art. The prior art only suggests forming multiple SSL connections wherein the CA certificate including all components access to the private key and a public key exist in each instance of forming such connections which however in so doing would violate the SSL paradigm in the case of performing data optimization operations between a server and client.

In contrast, the instant invention does not transmit the private key to preserve the SSL paradigm and yet enables optimization techniques to be performed through the second SSL connection between the client and server by

virtue of terminating the SSL connection at the client using the credentials of the web server but without transferring the private key over to the client.

Stampede Technologies, Inc. set out to reduce traffic over the network and increase the speed in which data is transmitted over the network when faced with an environment using single SSL connections between the same client server pairing.

In Conclusion

There is no disclosure, suggestion or teaching in Aziz as to the need or means for making multiple SSL connections with the same client and server. Nor is there any disclosure, teaching or suggestion of the claimed invention.

Gast is directed to a system and method for accelerating cryptographically secured transactions. Applicants assert Gast teaches away from the instant invention. It is recognized that teaching away requires discouragement of the invention. What a reference teaches or suggests must be examined in the context of knowledge, skill and reasoning ability of a skilled artisan. Gast recognizes the problem of encryption latency, paragraph [0015] of Gast. This latency can be encountered between a client server relationship. Gast chooses to offload the cryptographic process to central cryptographic hardware component employing an intermediary device to deal with the issue as opposed to creating an additional potential encryption latency issue between a server and client.

The concept presented by the instant invention is in creating multiple SSL

direct connections between the same client and server is discouraged by the prior art with the recognition of such connections causing encryption latency issues. Further, there is no teaching of how to create such direct multiple SSL connections between the same client and server in a manner to enhance performance and deal with latency issues directly between the same client and server employing a given CA certificate and a pseudo copy thereof.

Aziz attempts to teach toward offloading the SSL connection by using a cleartext HTTP connection, i.e., Aziz states this reduces the server workload even more compared to using previously negotiated SSL sessions." Combining the references in no way would result in the present invention. In fairly interpreting the teachings of each reference and combining such teachings, a reasonable combination might result in the combination of offloading encryption processing further with the aid of relays. This does not render the instant invention.

Like Aziz, in Freed et al. there is no direct link between the client computer and the server computer. Freed merely uses conventional SSL handshake which is employed and all secure data is sent through the one secure tunnel which is created. Freed et al. are concerned with offloading the server the task of encryption/decryption task by employing a tertiary or intermediary device to interact with the client and the server. The tertiary computer employs conventional handshake technology.

This is very different from the instant invention. The instant invention

provides a server with SSL protocol server software and SSL acceleration server software on both the client and server for enabling direct and multiple SSL sessions to take place through the use of creating a pseudo CA certificate on the web server in addition to having the existing CA certificate on the web server which are presented to the client computer having SSL protocol and SSL acceleration software thereon. By so providing, multiple direct secure links are created.

The instant invention enables secure data be transacted using the CA certificate from the web server over an initial SSL connection for transacting key data which must pass over such connection, such as when connecting to a secure bank site, for example. In addition, the instant invention provides the pseudo CA certificate and secondary SSL connection through which data may pass in a secure connection which enables functional operations (optimization techniques) to be performed thereon, such as compression of data. This is not taught, disclosed or suggested in Freed et al. (or Aziz) and this can't be accomplished in the teachings of Freed et al or Aziz. Freed et al. only acts as an intermediary intercepting all communication over the existing SSL connection and passes the data accordingly are only concerned with providing a classic SSL connection between the client and server through an intermediary device. There is no reasonable basis in which the references can be construed to teach, suggest or disclose the instant invention.

The issue is here is whether Aziz, Gast nor Freed et al. and some other

knowledge (presumably the Examiner's) brought here together renders obvious claimed invention. The Federal Circuit has followed the Court's holding in Adams. See, e.g., Kahn v. General Motors Corp., 135 F.3d 1472, 1479-80 (Fed. Cir. 1998), cert. denied, 525 U.S. 875 (1998) ("In determining obviousness, the invention must be considered as a whole.").

The differences between the prior art and claimed invention are very apparent, i.e., enabling secure data be transacted using the CA certificate from the web server over an initial SSL connection for transacting key data which must pass over such connection, and providing the pseudo CA certificate and secondary SSL connection through which data may pass in a secure connection which enables functional operations (optimization techniques) to be performed thereon. The level of ordinary skill in the art in the field of field has not been established or demonstrated by the examiner and cannot be asserted without some reasonable basis for doing so. Finally, while secondary considerations were not vigorously stressed in the prosecution of the application, it is noted that the applicant's invention has enjoyed much commercial success and is of wide spread need in the industry.

The instant invention is respectfully submitted to be patentably distinct over the art of record. Reversal of the rejection of the rejection of claims 1, 2, 9, 11, 12, 19, 24, 25 and 26 under 35 U.S.C. 103 over Aziz in view of Gast and/or Freed et al. and allowance of claims 1, 2, 9, 11, 12, 19, 24, 25 and 26 are respectfully requested.

Respectfully submitted,

/R. William Graham/

R. William Graham

Reg. No. 33,891

Certificate of transmission

I hereby certify that this Appeal Brief is being electronically filed with the Commissioner of Patent and Trademarks, Washington, D.C. 20231on the date shown below.

Date. August 17, 2010

R. William Graham

VIII. CLAIMS APPENDIX A (37 CFR 41.37(c)(1)(viii)

Unentered Claims

1. (Currently amended) A system for increasing data access in a secure socket layer network environment, which includes:

a web server computer having SSL protocol server software operably associated therewith for enabling a first SSL connection, wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with said web server computer which includes a pseudo CA certificate and access to said private key and a public key; and

a client computer communicatively linked to said web server computer having web browser software having SSL protocol client software operably disposed thereon ~~residing with~~ for enabling said first SSL connection between said client computer and said web server, wherein said first SSL connection is established between said web browser software and SSL acceleration client software operably disposed thereon ~~residing with~~ said client computer, wherein said SSL acceleration client software communicates with said SSL acceleration server software to receive a copy of said pseudo CA certificate and said public key and present said pseudo CA certificate to said web browser software for validation thereof for enabling a second SSL connection with said first SSL

connection between said client computer and said web server computer, wherein said second SSL connection is established between said SSL acceleration client software and said SSL acceleration server software in a manner wherein said private key is never transmitted to the SSL acceleration client software on said client computer and which permits optimization techniques to be applied on data transmitted through said second SSL connection.

2. (Previously presented) The system of claim 1, wherein said SSL acceleration client software is further equipped for monitoring when said web browser requests said first SSL connection with said web server computer and intercepting said SSL request from said web browser, and diverting communication through said second SSL connection.

3. (Cancelled).

4. (Cancelled).

5. (Cancelled).

6. (Cancelled).

7. (Cancelled).

8. (Cancelled).

9. (Previously presented) The system of claim 1, which includes compression software for transmitting data secure communications between said client computer and said web server computer over said second SSL connection.

10. (Cancelled).

11. (Currently amended) A method for increasing data access in a secure socket

layer network environment, which includes the steps of:

employing a web server computer having SSL protocol server software operably associated therewith for enabling a first SSL connection, wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with said web server computer which includes a pseudo CA certificate and access to said private key and a public key; and

employing a client computer communicatively linked to said web server computer having web browser software having SSL protocol client software operably disposed thereon ~~residing with~~ for enabling said first SSL connection between said client and said web server, wherein said first SSL connection is established between said web browser software and SSL acceleration client software operably disposed thereon ~~residing with~~ said client computer, wherein said SSL acceleration client software communicates with said SSL acceleration server software to receive a copy of said pseudo CA certificate and said public key and present said pseudo CA certificate to said web browser software through SSL acceleration server software for validation thereof for enabling a second SSL connection with said first SSL connection between said client computer and said web server computer, wherein said second SSL connection is established between said SSL acceleration client software and said SSL acceleration server software in a manner wherein said private key is never transmitted to the SSL acceleration client software on said client computer and which permits

optimization techniques to be applied on data transmitted through said second SSL connection.

12. (Previously presented) The method of claim 11, wherein said SSL acceleration monitors when said web browser requests said first SSL connection with said web server computer and intercepts said SSL request from said web browser, and diverts communication through said second SSL connection.

13. (Cancelled).

14. (Cancelled).

15. (Cancelled).

16. (Cancelled).

17. (Cancelled).

18. (Cancelled).

19. (Previously presented) The method of claim 11, which includes employing compression software for transmitting data secure communications between said client computer and said web server computer over said second SSL connection.

20. (Cancelled).

21. (Cancelled).

22. (Cancelled).

23. (Cancelled).

24. (Currently amended) A system for increasing data access in a secure socket layer network environment, which includes:

a web server computer having SSL protocol server software operably

associated therewith for enabling a first SSL connection, wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with said web server computer which includes a pseudo CA certificate and access to said private key and a public key; and

a second computer communicatively linked to said web server computer operably associated with web browser software having SSL protocol client software operably disposed thereon ~~residing therewith~~ for enabling said first SSL connection between a client computer and said web server, wherein said first SSL connection is established between said web browser software and SSL acceleration client software operably disposed thereon ~~residing~~ said second computer, wherein said SSL acceleration client software communicates with said SSL acceleration server software to receive a copy of said pseudo CA certificate and said public key and present said pseudo CA certificate to said web browser software for validation thereof for enabling a second SSL connection with said first SSL connection between said client computer and said web server computer, wherein said second SSL connection is established between said SSL acceleration client software and said SSL acceleration server software in a manner wherein said private key is never transmitted to said SSL acceleration client software and which permits optimization techniques to be applied on data transmitted through said second SSL connection.

25. (Previously presented) The system of claim 24, wherein said SSL acceleration client software is further equipped for monitoring when said web

browser requests said first SSL connection with said web server computer and intercepting said SSL request from said web browser, and diverting communication through said second SSL connection.

26. (Previously presented) The system of claim 24, which includes compression software for transmitting data secure communications between said client computer and said web server computer over said second SSL connection.

LISTING OF CLAIMS AS CURRENTLY STAND

1. (Previously presented) A system for increasing data access in a secure socket layer network environment, which includes:

a web server computer having SSL protocol server software operably associated therewith for enabling a first SSL connection, wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with said web server computer which includes a pseudo CA certificate and access to said private key and a public key; and

a client computer communicatively linked to said web server computer having web browser software having SSL protocol client software operably residing therewith for enabling said first SSL connection between said client computer and said web server, wherein said first SSL connection is established between said web browser software and SSL acceleration client software operably residing with said client computer, wherein said SSL acceleration client software communicates with said SSL acceleration server software to receive a copy of said pseudo CA certificate and said public key and present said pseudo CA certificate to said web browser software for validation thereof for enabling a second SSL connection with said first SSL connection between said client computer and said web server computer, wherein said second SSL connection is established between said SSL acceleration client software and said SSL

acceleration server software in a manner wherein said private key is never transmitted to the SSL acceleration client software on said client computer and which permits optimization techniques to be applied on data transmitted through said second SSL connection.

2. (Previously presented) The system of claim 1, wherein said SSL acceleration client software is further equipped for monitoring when said web browser requests said first SSL connection with said web server computer and intercepting said SSL request from said web browser, and diverting communication through said second SSL connection.

3. (Cancelled).

4. (Cancelled).

5. (Cancelled).

6. (Cancelled).

7. (Cancelled).

8. (Cancelled).

9. (Previously presented) The system of claim 1, which includes compression software for transmitting data secure communications between said client computer and said web server computer over said second SSL connection.

10. (Cancelled).

11. (Previously presented) A method for increasing data access in a secure socket layer network environment, which includes the steps of:

employing a web server computer having SSL protocol server software

operably associated therewith for enabling a first SSL connection, wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server software operably associated with said web server computer which includes a pseudo CA certificate and access to said private key and a public key; and

employing a client computer communicatively linked to said web server computer having web browser software having SSL protocol client software operably residing therewith for enabling said first SSL connection between said client and said web server, wherein said first SSL connection is established between said web browser software and SSL acceleration client software operably residing with said client computer, wherein said SSL acceleration client software communicates with said SSL acceleration server software to receive a copy of said pseudo CA certificate and said public key and present said pseudo CA certificate to said web browser software through SSL acceleration server software for validation thereof for enabling a second SSL connection with said first SSL connection between said client computer and said web server computer, wherein said second SSL connection is established between said SSL acceleration client software and said SSL acceleration server software in a manner wherein said private key is never transmitted to the SSL acceleration client software on said client computer and which permits optimization techniques to be applied on data transmitted through said second SSL connection.

12. (Previously presented) The method of claim 11, wherein said SSL acceleration monitors when said web browser requests said first SSL connection with said web server computer and intercepts said SSL request from said web browser, and diverts communication through said second SSL connection.

13. (Cancelled).

14. (Cancelled).

15. (Cancelled).

16. (Cancelled).

17. (Cancelled).

18. (Cancelled).

19. (Previously presented) The method of claim 11, which includes employing compression software for transmitting data secure communications between said client computer and said web server computer over said second SSL connection.

20. (Cancelled).

21. (Cancelled).

22. (Cancelled).

23. (Cancelled).

24. (Previously presented) A system for increasing data access in a secure socket layer network environment, which includes:

a web server computer having SSL protocol server software operably associated therewith for enabling a first SSL connection, wherein SSL protocol server software includes a CA certificate and private key, SSL acceleration server

software operably associated with said web server computer which includes a pseudo CA certificate and access to said private key and a public key; and

a second computer communicatively linked to said web server computer operably associated with web browser software having SSL protocol client software operably residing therewith for enabling said first SSL connection between a client computer and said web server, wherein said first SSL connection is established between said web browser software and SSL acceleration client software operably residing said second computer, wherein said SSL acceleration client software communicates with said SSL acceleration server software to receive a copy of said pseudo CA certificate and said public key and present said pseudo CA certificate to said web browser software for validation thereof for enabling a second SSL connection with said first SSL connection between said client computer and said web server computer, wherein said second SSL connection is established between said SSL acceleration client software and said SSL acceleration server software in a manner wherein said private key is never transmitted to said SSL acceleration client software and which permits optimization techniques to be applied on data transmitted through said second SSL connection.

25. (Previously presented) The system of claim 24, wherein said SSL acceleration client software is further equipped for monitoring when said web browser requests said first SSL connection with said web server computer and intercepting said SSL request from said web browser, and diverting

communication through said second SSL connection.

26. (Previously presented) The system of claim 24, which includes compression software for transmitting data secure communications between said client computer and said web server computer over said second SSL connection.

X. EVIDENCE APPENDIX (37 CFR 41.37(c)(1)(ix))

There is no additional evidence presented.

IX. RELATED PROCEEDINGS APPENDIX (37 CFR 41.37(c)(1)(x)

There are no related proceedings.